ОТЗЫВ

на автореферат диссертации Лелюка Евгения Андреевича
«Синтез постквантовой схемы инкапсуляции сеансового ключа»,
представленной на соискание ученой степени кандидата технических наук
по специальности 2.3.6 – «Методы и системы защиты информации,
информационная безопасность»

Диссертационная работа Е.А. Лелюка посвящена исследованию кодовых схем шифрования для использования в протоколах безопасной передачи секретного ключа по незащищённому каналу. Актуальность темы обусловлена т. н. «квантовой угрозой» - возможностью решения за полиномиальное время задач факторизации и дискретного логарифмирования, на сложности которых в настоящее время основана стойкость большинства асимметричных криптосистем; для кодовых криптосистем подобных атак с применением квантового компьютера пока не известно.

В работе предложена и исследована криптосистема типа Мак-Элиса на конструкции *D*-кодов, а именно: разработаны алгоритмы шифрования и расшифрования; описан способ определения сильных и слабых ключей криптосистемы; предложена и реализована комбинированная атака на криптосистему в случае использования слабых ключей; получены параметры, гарантирующие стойкость предложенной криптосистемы к структурной атаке. Все математические результаты оформлены в виде теорем и строго доказаны.

Практическая значимость работы подтверждена многочисленными экспериментальными данными, которые, в частности, свидетельствуют о преимуществе построенной криптосистемы на *D*-кодах перед оригинальной системой, основанной на кодах Гоппы: она обладает большей стойкостью при сопоставимых размерах ключа либо обеспечивает тот же уровень стойкости, но при ключах меньшего размера.

Считаю, что диссертация соответствует требованиям «Положения о порядке присуждения учёных степеней», а её автор Лелюк Евгений Андреевич достоин присуждения учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Панкратова Ирина Анатольевна
зав. лабораторией компьютерной криптографии
федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский государственный университет»,
кандидат физико-математических наук по специальности 05.13.01 — Управление в технических системах, доцент

634050, г. Томск, пр. Ленина, 36.
Тел. +7 (3822)-529-852
E-mail: rector@tsu.ru

14 апреля 2026 года

ПОДПИСЬ УДОСТОВЕРЯЮ
ВЕДУЩИЙ ДОКУМЕНТОВЕД
АНДРИЕНКО И.В.